AF
SRW

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Appellant:	**Graeme John PROUDLER et al.**	Examiner:	Tri H. PHAN
Serial No.:	**09/913,453**	Art Unit:	2661
Filed:	August 14, 2001	Our Ref:	B-4276PCT 619003-1 30990088-3 US
For:	"COMMUNICATIONS BETWEEN MODULES OF A COMPUTING APPARATUS"	Date:	June 13, 2006
		Re:	***Appeal to the Board of Appeals***

BRIEF ON APPEAL

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This is an appeal from the Final rejection, dated December 13, 2005, for the above identified patent application. Appellants submit that this Appeal Brief is being timely filed because the Notice of Appeal was filed on April 13, 2006. Please deduct the amount of $500.00 for the fee set forth in 37 C.F.R. 1.17(c) for submitting this Brief from deposit account no. 08-2025.

REAL PARTY IN INTEREST

The real party in interest to the present application is Hewlett-Packard Development Company, LP, a limited partnership established under the laws of the State of Texas and having a principal place of business at 20555 S.H. 249 Houston, TX 77070, U.S.A. (hereinafter "HPDC"). HPDC is a Texas limited partnership and is a wholly-owned affiliate of Hewlett-Packard Company, a Delaware Corporation, headquartered in Palo Alto, CA. The general or managing partner of HPDC is HPQ Holdings, LLC.

RELATED APPEALS AND INTERFERENCES

There are no other appeals or interferences related to the present application.

STATUS OF CLAIMS

Claims 1 - 30 are the subject of this Appeal and are reproduced in the accompanying appendix.

STATUS OF AMENDMENTS

No Amendment After Final Rejection has been entered.

SUMMARY OF CLAIMED SUBJECT MATTER

The invention described and claimed in the present application relates generally to improving trust and security between various modules of a computing apparatus (p. 1 ll. 1-2). Claim 1 in particular is directed to a computing apparatus comprising a trusted hardware module (p. 8 l. 29), a plurality of further hardware modules (p. 8 ll. 27-32), a shared communication infrastructure by which the hardware modules can communicate with each other (p. 17 ll. 26-28), and a first communication path, distinct from the shared communication infrastructure, by which a first one of the further hardware modules can communicate directly with the trusted hardware module but cannot communicate directly with any other of the further hardware modules (p. 18 ll. 6-16).

Claims 21 is directed to a computing apparatus comprising a trusted hardware module resistant to unauthorized modification (p. 8 l. 29), a plurality of further hardware modules (p. 8 ll. 27-32), a shared communication infrastructure by which the hardware modules can communicate with each other (p. 17 ll. 26-28), and a first communication path distinct from the shared communication infrastructure by which a first one of the further hardware modules can communicate directly with the trusted hardware module but which is inaccessible to the other further hardware modules (p. 18 ll. 6-16).

It is important to understand at the outset that the claims cover just what they state: an apparatus, that is, an *appliance* or *device* for a particular purpose (The American Heritage® Dictionary of the English Language, Fourth Edition. Houghton Mifflin Company, 2004). It will

further aid Appellant's presentation to also note at the outset that an appliance or device is not a network. "Network: group or system of electric components and connecting circuitry designed to function in a specific manner." *Ibid.*

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Issue 1: Whether claims 1-3, 5-6, 13, 18, 21-23 and 25-26 are unpatentable under 35 U.S.C. 102(b) for being anticipated by U.S. Patent No. 5,822,435 to Boebert et al.

Issue 2: Whether claims 4, 7-12, 14-17, 19-20, 24 and 27-30 are unpatentable under 35 U.S.C. 103(a) for being obvious in view of Boebert.

GROUPING OF CLAIMS

For each ground of rejection which Appellant contests herein and which applies to more than one claim, such additional claims, to the extent separately identified and argued below, do not stand or fall together.

ARGUMENT

Issue 1: Whether claims 1-3, 5-6, 13, 18, 21-23 and 25-26 are unpatentable under 35 U.S.C. 102(b) for being anticipated by U.S. Patent No. 5,822,435 to Boebert et al.

In section 4 of the final Office Action of December 13, 2005, the Examiner once again rejects claims 1-3, 5-6, 13, 18, 21-23 and 25-26 under 35 U.S.C. 102(b) as being anticipated by U.S. Patent No. 5,822,435 to Boebert et al. In particular, the Examiner reiterates his opinion that, with regard to claims 1 and 21, Boebert discloses all of the claimed limitations.

In their reply of September 23, 2005, Appellants had explained why they respectfully disagree with the Examiner's opinion. In particular, Appellants explained that, *inter alia*, claims 1 and 21 both recite a shared communications infrastructure by which the hardware modules can communicate with each other, and a first communication path that is distinct from the shared communication infrastructure and by which a hardware module can communicate directly with the trusted hardware module but cannot communicate directly with any other of the hardware modules. Appellants further explained why the Examiner's assertion that such a shared

communications infrastructure is disclosed by Boebert in the "paths 44, 46 which connect the workstation processing unit to the display/video manager, keyboard/keyboard manager" is clearly at odds with the plain disclosure of Boebert.

Specifically, what the Examiner termed "paths 44, 46" are shown in both Fig. 1 (which shows a prior art system) and Figs. 2-5 (which show embodiments of Boebert's invention) and are described at col. 2, ll. 3-4, as a "video port" and "keyboard port" respectively. No person skilled in the art could possibly understand a video or keyboard port as corresponding to a shared communication infrastructure, especially in view of the figures of Boebert which clearly show both elements 44 and 46 as straight lines or paths between two components only. Appellants further noted that labels 44 and 46 appear to be used for different paths in the different figures but that, nonetheless, they are always shown as connecting two devices only, and that there is simply nothing in Boebert that could be understood as teaching that either of element 44 or 46 comprise a shared communication infrastructure. Such a structure is described in Appellants' specification by conventional communication paths 110 (examples for which are given as ISA, EISA, PCI, and USB paths) which are well known by those skilled in the art to refer to communication buses that connect a plurality of components of a computing platform.

In the final Action, the Examiner dismisses Appellants' discussion as not persuasive, and alleges to explain by offering that "In Figure 2 (or in figure 1), Boebert clearly discloses the connection between the workstation processing unit 40 to the multilevel secure computer 60, through the network 50, which is the shared communications connection where the hardware modules such as display, keyboard, workstation processing unit, ... can communicate to the trusted and untrusted subsystem of the multilevel secure computer, e.g. '*a shared communication infrastructure by which the hardware modules can communicate with each other.*'" With all due respect, this does not even make sense.

Appellants' claims are directed a computing apparatus, that is, a single device. The Examiner relies on Boebert's showing of two separate devices connected by a network as anticipating the present invention. This is simply untenable. The network 50 connects one device, the workstation processing unit 40, to another device, the multilevel secure computer 60 – this much is true. This, however, does not anticipate the claimed shared communications

infrastructure by which the hardware modules of an apparatus can communicate with each other, and a first communication path that is distinct from the shared communication infrastructure and by which a hardware module can communicate directly with the trusted hardware module but cannot communicate directly with any other of the hardware modules. Stretching the Examiner's proffered "explanation" to the outermost bounds of logic, Appellants can only understand him to allege that workstation processing unit 40 is a hardware module of an apparatus and the multilevel secure computer 60 is another hardware module of the selfsame apparatus, and that the network 50 is the shared communication infrastructure. This is patently incorrect. If the network 50 is a shared communication infrastructure, what is it shared by? All the other modules (display 10, keyboard 20, etc.) are clearly with no connection to this "shared" communication infrastructure, i.e. the network 50. Network 50 is clearly a *direct* path between two separate apparatuses – it is not a shared communication infrastructure of an apparatus.

Furthermore, Appellants note that the Examiner's "explanation" is directly at odds with his own earlier (and presently repeated) allegation that it is "paths 44, 46" that disclose the claimed shared communication infrastructure. Appellants thus feels compelled to inquire: which one is it, network 50 or paths 44, 46?

As fully detailed above, Appellants submit that claims 1 and 21 are in fact novel and patentable over the art of record, because Boebert does not disclose each and every claim limitation, and thus respectfully requests the Board to overturn the Examiner on appeal and pass these claims to allowance.

Claims 2-3, 5-6, 13, 18, 22-23 and 25-26 depend from claim 1 or 21. In view of the above discussion, wherein it is submitted that claims 1 and 21 are allowable, Appellants submit that claims 2-3, 5-6, 13, 18, 22-23 and 25-26 are also allowable at least by reason of their dependency.

Issue 2: Whether claims 4, 7-12, 14-17, 19-20, 24 and 27-30 are unpatentable under 35 U.S.C. 103(a) for being obvious in view of Boebert.

In section 5 of the final Office Action the Examiner once again rejects claims 4, 7-12, 14-17, 19-20, 24 and 27-30 under 35 U.S.C. 103(a) as being unpatentable over Boebert. Appellants

once again note that these claims depend from claim 1 or 21. "If an independent claim is nonobvious under 35 U.S.C. 103, then any claim depending therefrom is nonobvious." *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988). Therefore, in light of the above discussion of claims 1 and 21, Appellants submit that claims 4, 7-12, 14-17, 19-20, 24 and 27-30 are also allowable at least by reason of their dependency.

In view of all of the preceding, Appellants respectfully submit that all pending claims as pending are novel and nonobvious over the art of record and that the Examiner's rejection is not supported by the art, and thus request that the rejection of all claims be overturned on appeal and the case be passed to allowance.

CONCLUSION

For the extensive reasons advanced above, Appellants respectfully contend that each claim is patentable. Therefore, reversal of all rejections and allowance of the case is respectfully solicited.

I hereby certify that this correspondence is being deposited with the United States Post Service with sufficient postage as first class mail in an envelope addressed to: Mail Stop Appeal Brief-Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on

June 13, 2006
(Date of Transmission)

Alma Smalling
(Name of Person Transmitting)

(Signature)

6/13/06
(Date)

Respectfully submitted,

Robert Popa
Attorney for Appellants
Reg. No. 43,010
LADAS & PARRY
5670 Wilshire Boulevard, Suite 2100
Los Angeles, California 90036
(323) 934-2300 voice
(323) 934-0202 facsimile
rpopa@ladasparry.com

Attachments

Claims

1. (Previously Presented) A computing apparatus comprising:

a trusted hardware module;

a plurality of further hardware modules;

a shared communication infrastructure by which the hardware modules can communicate with each other; and

a first communication path, distinct from the shared communication infrastructure, by which a first one of the further hardware modules can communicate directly with the trusted hardware module but cannot communicate directly with any other of the further hardware modules.

2. (Previously Presented) An apparatus as claimed in claim 1, wherein the trusted hardware module and the first further hardware module each include a respective computing engine which partakes in the direct communication via the first communication path.

3. (Previously Presented) An apparatus as claimed in claim 2, wherein:

the first further hardware module is operable to supply to the trusted hardware module a request for operation on data; and

in response to such a request, the trusted hardware module is operable to generate a response and to supply the response to the first further hardware module via the first communication path and not via the shared communication infrastructure.

4. (Previously Presented) An apparatus as claimed in claim 3, wherein the trusted hardware module includes means for storing policy information regarding such operations which can or cannot be permitted, and is operable to generate the response with reference to the policy information.

5. (Previously Presented) An apparatus as claimed in claim 1, wherein the trusted hardware module is operable to generate an encryption and/or decryption key and to supply that key to the first further hardware module via the first communication path and not via the shared communication infrastructure.

6. (Previously Presented) An apparatus as claimed in claim 5, wherein the first further hardware module is operable to use the key for encryption and/or decryption of data communicated via the shared communication infrastructure.

7. (Previously Presented) An apparatus as claimed in claim 1,

wherein the trusted hardware module is operable to generate a challenge and to supply the challenge to the first further hardware module via the first communication path or via the shared communication infrastructure using encryption set up using the first communication path.

8. (Previously Presented) An apparatus as claimed in claim 7, wherein:

in response to the challenge, the first further hardware module is operable to generate a response and to supply the response to the trusted hardware module via the first communication path or via the shared communication infrastructure using encryption set up using the first communication path; and

the trusted hardware module is operable to use the response in generating an integrity metric of the apparatus.

9. (Previously Presented) An apparatus as claimed in claim 1, wherein:

the first further hardware module has a zone for private data and a zone for non-private data; and

the first further hardware module is operable to supply and/or receive data from/for the private data zone via the first

communication path and not via the shared communication infrastructure.

10. (Previously Presented) An apparatus as claimed in claim 9, wherein the first further hardware module is operable to supply and/or receive data from/for the non-private data zone via the shared communication infrastructure.

11. (Previously Presented) An apparatus as claimed in claim 10, wherein the first further hardware module has an interface between the private and non-private data zones which is operable to inhibit the passing of data from the private data zone to the non-private data zone.

12. (Previously Presented) An apparatus as claimed in claim 1, wherein the first further hardware module is a network interface module.

13. (Previously Presented) An apparatus as claimed in claim 1, and including a second communication path, distinct from the shared communication infrastructure and the first communication path, by which a second one of the further hardware modules can communicate directly with the trusted hardware module but cannot

communicate directly with any other of the further hardware modules.

14. (Previously Presented) An apparatus as claimed in claim 13, wherein:

the first further hardware module is operable to supply to the trusted hardware module a request for a transfer of data between the first and second further hardware modules; and

in response to such a request, the trusted hardware module is operable to generate a response and to supply the response to the first or second further hardware module via the first or second communication path, respectively, and not via the shared communication infrastructure.

15. (Previously Presented) An apparatus as claimed in claim 14, wherein the trusted hardware module includes means for storing policy information regarding such transfers which can or cannot be permitted, and is operable to generate the response with reference to the policy information.

16. (Previously Presented) An apparatus as claimed in claim 14, wherein:

in response to an appropriate such transfer response, the

first or second further hardware module is operable to supply the data to the trusted hardware module via the first or second communication path, as the case may be; and

in response to the receipt of such data, the trusted hardware module is operable to relay the data to the second or first further hardware module, respectively, via the second or first communication path, as the case may be.

17. (Previously Presented) An apparatus as claimed in claim 13, wherein the second further hardware module is a main processor unit of the apparatus or a non-volatile data storage module.

18. (Previously Presented) An apparatus as claimed in claim 13, and including at least a third communication path, distinct from the shared communication infrastructure and the other communication paths, by which at least a third one of the further hardware modules can communicate directly with the trusted hardware module but cannot communicate directly with any other of the further hardware modules.

19. (Previously Presented) An apparatus as claimed in claim 18, wherein the second further hardware module is a main

processor unit of the apparatus and the third further hardware module is a non-volatile data storage module.

20. (Previously Presented) An apparatus as claimed in claim 1, wherein the trusted hardware module is adapted to measure an integrity metric of the computing apparatus.

21. (Previously Presented) A computing apparatus comprising:

a trusted hardware module resistant to unauthorized modification;

a plurality of further hardware modules;

a shared communication infrastructure by which the hardware modules can communicate with each other; and

a first communication path distinct from the shared communication infrastructure by which a first one of the further hardware modules can communicate directly with the trusted hardware module but which is inaccessible to the other further hardware modules.

22. (Previously Presented) An apparatus as claimed in claim 21, wherein the trusted hardware module and the first further hardware module each include a respective computing engine which partakes in the direct communication via the first communication

path.

23. (Previously Presented) An apparatus as claimed in claim 22, wherein:

the first further hardware module is operable to supply to the trusted hardware module a request for operation on data; and

in response to such a request, the trusted hardware module is operable to generate a response and to supply the response to the first further hardware module via the first communication path and not via the shared communication infrastructure.

24. (Previously Presented) An apparatus as claimed in claim 23, wherein the trusted hardware module includes means for storing policy information regarding such operations which can or cannot be permitted, and is operable to generate the response with reference to the policy information.

25. (Previously Presented) An apparatus as claimed in claim 21, wherein the trusted hardware module is operable to generate an encryption and/or decryption key and to supply that key to the first further hardware module via the first communication path and not via the shared communication infrastructure.

26. (Previously Presented) An apparatus as claimed in claim 25, wherein the first further hardware module is operable to use the key for encryption and/or decryption of data communicated via the shared communication infrastructure.

27. (Previously Presented) An apparatus as claimed in claim 21, wherein the trusted hardware module is operable to generate a challenge and to supply the challenge to the first further hardware module via the first communication path or via the shared communication infrastructure using encryption set up using the first communication path.

28. (Previously Presented) An apparatus as claimed in claim 27, wherein:

in response to the challenge, the first further hardware module is operable to generate a response and to supply the response to the trusted hardware module via the first communication path or via the shared communication infrastructure using encryption set up using the first communication path; and

the trusted hardware module is operable to use the response in generating an integrity metric of the apparatus.

29. (Previously Presented) An apparatus as claimed in claim 21, wherein the first further hardware module is a network interface module.

30. (Previously Presented) An apparatus as claimed in claim 21, wherein the trusted hardware module is adapted to measure an integrity metric of the computing apparatus.

There is no evidence submitted with the present Brief on Appeal.

There are no other appeals or interferences related to the present application.